SEALED

UNITED STATES DISTRICT COURT FOR THE
SOUTHERN DISTRICT OF WEST VIRGINIA
CHARLESTON

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FACEBOOK USER ACCOUNT "Rj Johnson" (Facebook UID 10004489370664) that is stored at premises controlled by Facebook, Inc., headquartered at 1601 Willow Road, Menlo Park, CA 94025	**Criminal No. 2:21-mj-00142** **Filed under seal**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Terrance L. Taylor, being duly sworn, do hereby depose and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been so employed since March 2012. I am currently assigned to the Office of the Resident Agent in Charge, HSI Charleston, West Virginia. During my career, I gained experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience—including on-the-job discussions with other law enforcement agents and cooperating suspects—I am familiar with the operational techniques and organizational structure of child pornography distribution networks as well as the traits and characteristics of child pornography collectors and possessors and their use of computers or other electronic and media devices to facilitate the collection, possession, trading, distribution, access and receipt of child pornographic materials.

2. I am a Special Agent with nineteen years of federal law enforcement experience. Prior to my employment with HSI, I was a Police Officer for two years in Huntington, West

Virginia, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years, and a Special Agent with the United States Department of State-Office of Inspector General for two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center ("FLETC") and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. These areas include laws and regulations pertaining to the importation of various types of merchandise and contraband, prohibited items, money laundering, and various immigration violations. I have more specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, and 2256.

II. PURPOSE OF THE AFFIDAVIT

3. The statements contained in this affidavit are based on my knowledge or information provided by Facebook and the National Center for Missing and Exploited Children ("NCMEC"). This affidavit is being submitted for the limited purpose of securing a search warrant and, accordingly, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts necessary to establish probable cause that violations of Title 18, United States Code, § 2252A(a)(5)(B), possession of child pornography; 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and § 2252A(a)(1), the transportation of child pornography in interstate commerce, have occurred

in Clay County, West Virginia, within the Southern District of West Virginia, and that evidence of those violations is presently stored at the premises owned, controlled or operated by Facebook, Inc. an electronic service provided headquartered at 1601 Willow Road, Menlo Park, CA 94025.

III. STATUTORY AUTHORITY

4. The investigation concerns potential violations of 18 U.S.C. §§ 2252A(a)(1), (2), and (5)(B), relating to matters involving the sexual exploitation of minors.

a. **18 U.S.C. 2252A (a)(1)** prohibits any person from knowingly mailing, transporting, or shipping child pornography in interest or foreign commerce by any means, including by computer.

b. **18 U.S.C. § 2252A(a)(2)** prohibits any person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

c. **18 U.S.C § 2252A(a)(5)(B)** prohibits any person from knowingly possessing any book, magazines, periodicals films, video tapes computer disk or other matter that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means including computer, or that was produced using materials mailed, or shipped or transported in interstate or foreign commerce by any means including computer.

IV. DEFINITIONS

5. The following definitions apply to this Affidavit and its Attachments.

a. The term **"minor,"** as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term **"sexually explicit conduct,"** as used in 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term "**illicit sexual conduct**" means (1) a sexual act (as defined in section 2246) with a person under 18 years of age that would be a violation of chapter 109A if the sexual act occurred in the special maritime and territorial jurisdiction of the United States; or (2) any commercial sex act (as defined in section 1591) with a person under the age of 18 years of age.

d. The term "**visual depiction**," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

e. The term "**computer**," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

f. The term "**child pornography**," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where

i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

iii. such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

g. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact disks, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

h. **"Internet Service Providers"** (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-locations of computers and other communications equipment.

i. **"Internet Protocol address"** (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can by dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static if an ISP assigns a user's computer a particular IP address each time the computer accesses the Internet.

j. **"Domain names"** are common, easy to remember names associated with an IP address. For example, a domain name of www.usdoj.gov refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

k. **"Website"** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

V. JURISDICTION

6. The legal authority for this search warrant application is derived from 18 U.S.C. §§ 2701-2711. 18 U.S.C. § 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703, a government entity may require a provider of an electronic communication service or a remote computing service to

disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation.

7. This Court has jurisdiction to issue the requested warrant as it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is "a district court of the United States (including a magistrate judge or such a court) . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). The investigation reveals that the target, Robert JOHNSON, engaged in illegal conduct, as referenced in this Affidavit, from and within the Southern District of West Virginia. See 18 U.S.C. § 3237; see also 18 U.S.C. §§ 3231 and 3232.

VI. BACKGROUND REGARDING COMPUTERS, CHILD PORNOGRAPHY AND THE INTERNET

8. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). Darkroom facilities and a significant amount of skill were required in order to develop and reproduce the photographic images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their detection by the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children.

Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Child pornographers can now transfer photographs from a camera in a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem.[1] Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials among pornographers.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has increased tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Inc. and Google, Inc., among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can often be found on the user's computer.

---

[1] The File Transfer Protocol ("FTP") is a protocol that defines how files are transferred from one computer to another. One example, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on the computer indefinitely until overwritten by other data.

VII. BACKGROUND ON THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN'S CYBERTIPLINE

9. Based on my training and experience, and publicly-available information, I know that the National Center for Missing and Exploited Children ("NCMEC") is a nonprofit, nongovernmental organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

10. In addition to reports from the general public, Title 18, United States Code, Section 2258A requires all providers of an electronic communication service or remote computing service to the public through a facility or means of interstate or foreign commerce, known as electronic service providers ("ESPs"), to report "apparent child pornography" to NCMEC via the CyberTipline. Leads received by NCMEC are reviewed by specially-trained analysts, who examine and evaluate the reported content, add related information that may be useful to law

enforcement, use publicly-available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation. In this case, the ESP was Facebook and it made a CyberTipline referral ("CyberTip") to NCMEC based on the conduct described below.

11. Thus, NCMEC received CyberTips on the following types of criminal conduct: possession, manufacture and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

12. CyberTips can vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an electronic communication service or remote commuting service uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography. See 18 U.S.C. § 2258A(b). Also, as will be illustrated below, CyberTips can be supplemented and made in connection with other CyberTips.

VIII. BACKGROUND ON FACEBOOK

13. Facebook is a social networking company headquartered in Menlo Park, California, which owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public. Facebook is an electronic service provider ("ESP") that makes CyberTip referrals to NCMEC when it detects suspected criminal activity.

14. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

15. Facebook embeds associated accounts with "cookies" or "machine cookie" technology. Cookies are a small text file created by a website that is stored in the user's computer either temporarily for that session only or permanently on the hard drive. Cookies provide a way for the website (Facebook) to recognize a user and keep track of a user's preferences. This further allows Facebook to identify related or "linked" Facebook accounts (two different accounts for the same user) that are utilizing an assigned "machine cookie" when logged in.

16. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual

Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

17. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

18. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

19. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

20. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

21. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

22. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

23. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

24. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

25. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

26. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

27. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

28. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

29. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head

of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and/or administrator, as well as a PDF of the current status of the group profile page.

30. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

31. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile and would show when and from what IP address the user did so.

32. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may

communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

33. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element, or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and

Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

34. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

IX. CHARACTERISTICS OF PERSONS WHO COLLECT OR TRAFFIC CHILD PORNOGRAPHY

35. Your affiant has experience in assisting with, and leading, investigations into child pornography. Your affiant has conducted investigations into those who solicit and share child pornography by electronic means. Your affiant has worked with other law enforcement agencies to conduct logical investigations into those who solicit, share and otherwise engage in activity related to child pornography.

36. As a result of the aforementioned knowledge and experience, your affiant has learned that the characteristics described in Paragraphs 36-39 are generally found to exist in varying combinations and be true in cases involving offenders who send, cause to be sent, distribute, exhibit, possess, display, transport, manufacture or produce material which depicts minors engaged in sexually explicit conduct. Said material may include, but is not limited to,

photographs, negatives, slides, magazines, printed media, motion pictures, video tapes, books and other media stored electronically on computers, digital devices or related digital storage media.

37. Offenders who deal with the above-referenced child pornography material depicting minors engaged in sexually explicit conduct obtain or traffic in such materials through many sources and by several methods and means. These sources, methods and means include, but are not limited to, the following:

a. Downloading via the Internet and other computer networks (including from websites, peer-to-peer file sharing networks, news groups, electronic bulletin boards, chat rooms, instant message conversations, internet relay chats, email).

b. Receipt from commercial sources within and outside of the United States through shipments, deliveries and electronic transfer.

c. Trading with other persons with similar interests through electronic transfer, shipments or deliveries.

38. These offenders collect materials depicting minors engaged in sexually explicit conduct for many reasons. These reasons include the following:

a. For sexual arousal and sexual gratification.

b. To facilitate sexual fantasies in the same manner that other persons utilize adult pornography.

c. As a medium of exchange in return for new images and video depicting minors engaged in sexually explicit conduct.

39. These offenders often view their child pornographic materials as valuable commodities, sometimes even regarding them as prized collections. Subsequently, these offenders prefer not to be without their child pornographic material for any prolonged period of time and often go to great lengths to conceal and protect their illicit collections from discovery, theft or damage. To safeguard their illicit materials, these offenders may employ the following methods:

a. The use of Internet-based data storage services, such a Google Drive.

b. The use of labels containing false, misleading or no title.

c. The application of technologies, software and other electronic means such as encryption, steganography (the practice of concealing a file, message, image, or video within another file, message, image, or video), partitioned hard drives, and misleading or purposefully-disguised applications on electronic devices.

d. The use of safes, safety deposit boxes or other locked or concealed compartments within premises or structures that the offender controls.

X. FACTS ESTABLISHING PROBABLE CAUSE

40. On or about February 17, 2021, Facebook submitted CyberTip Report 86295910 to the NCMEC CyberTipline. The Cybertip Report was the result of Facebook representatives identifying that on or about December 21, 2020, a Facebook profile bearing the username "Rj Johnson" (and Facebook User ID 100044893370664) had uploaded one video file through Facebook messenger, which Facebook identified as a "hash match" to a previously identified video of a prepubescent minor engaged in sexual activity.

41. On or about March 22, 2021, NCMEC forwarded the above Cybertip report to the Virginia State Police who then forwarded it to the West Virginia State Police ("WVSP") because the report noted the Facebook login is associated to an AT&T Wireless subscriber from Maysel, Clay County, West Virginia. On June 11, 2021, the WVSP assigned that report to HSI WV for investigation.

42. On or about July 19, 2021, HSI Special Agent Michael D. Fleener obtained a search warrant to view the flagged media at issue, a video file, which was attached to the CyberTip but had not yet been reviewed by the ESP. On or about July 28, 2021, Special Agent Fleener reviewed the file and found it depict the following:

a. Alphanumeric file DRryEH8QVtEq8lkC132090425_726196088330083_6747844780978447898_n.mp4 depicts a 2:29 video of a prepubescent female with brown skin and black hair, approximately 9-11 years. The prepubescent female is nude and straddling an unknown white adult male whom is also nude and lying down on a bed. The adult male is penetrating the prepubescent female's vagina with his erect penis.

43. In Cybertip Report 86295910, Facebook reported that on or about December 21, 2020, Facebook user "Rj Johnson" uploaded one video file at approximately 05:36:16 UTC believed to be child pornography. The IP address associated with that Facebook account that was captured by Facebook at the time of upload was 2600:0387:000c:5712::146 and investigative records reflect that it is tied to an AT&T wireless cellphone. Facebook further noted in the CyberTip that the "Rj Johnson" account information at the time of the upload was as follows:

Name: Rj Johnson

Mobile Phone: XXXXXX2867

Date of Birth: XX-XXX-1966

Email: roj19661124@gmail.com (verified)

Age: 54

Screen Name: Rj Johnson

UID:100044893370664

44. In the CyberTip, Facebook provided the flagged video file uploaded by "Rj Johnson" that contained child pornography, plus a second image file that was being used as the accounts profile picture. The profile picture depicts a white male, approximately fifty to sixty years of age, with short gray hair. This file was publicly available to all Facebook users.

45. On or about June 2, 2021, the Virginia State Police (not the West Virginia State Police) issued an administrative subpoena to AT&T Internet Services for information relating to who the subscriber was for the phone number ending in -2867 (the phone number associated with the "RJ Johnson" Facebook account) on December 21, 2020 at 05:36 UTC (the time of the upload).

On or about June 4, 2021, representatives of AT&T Internet Services responded electronically advising that phone number ending in -2867 was associated to Account #418114564373 from October 1, 2020 through March 27, 2021. The records reflected that the billing party for that account was ROBERT JOHNSON, with a post office box ("P.O. Box") located in Maysel, West Virginia 25133. Maysel is a small, rural, unincorporated community in Clay County, West Virginia, within the Southern District of West Virginia.

46. Publicly available database checks reveal that an individual named ROBERT JOHNSON resides at a Clay Mountain Road address in Procious, West Virginia. Those same records also reveal that this same individual is associated with an Emergency-911 address on Hilltop Lane in Procious, West Virginia, and that he has a P.O. Box in Maysel, West Virginia, as a mailing address. The date of birth listed for JOHNSON matches the date of birth listed in the Facebook account information provided in the CyberTip.

47. A check with the West Virginia Department of Motor Vehicles ("DMV") reveals a ROBERT JOHNSON who is registered there with a P.O. Box in Maysel, West Virginia that matches the Maysel, West Virginia, mailing address referenced above in Paragraphs 45-46 for ROBERT JOHNSON. JOHNSON'S date of birth on file with the DMV matches the date of birth listed in the Facebook CyberTip. The DMV lists JOHNSON's West Virginia Driver's License as #XXXXX98. The image displayed on the Driver's License appears to be the same individual depicted in the Facebook profile picture described in Paragraph 44.

48. On or about June 16, 2021, Trooper Robert Cervera of the West Virginia State Police conducted surveillance at the Clay Mountain Road residence in Procious, West Virginia, which was described in Paragraph 46 as associated with JOHNSON. Trooper Cervera observed a grey Dodge Stratus bearing a West Virginia license plate that was parked in the driveway in front

of the residence, which appeared to be a single-family structure. The license plates and Dodge Stratus is registered to ROBERT JOHNSON at the same Maysel, West Virginia, P.O. Box referenced above in Paragraphs 46-47.

49. On or about June 16, 2021, HSI in West Virginia issued an administrative subpoena to American Electric Power Company ("AEP") regarding utility service at the Clay Mountain Road residence in Procious, West Virginia. AEP responded on June 21, 2021, and provided information that Account 024-229-536-8 is assigned to "ROBERT O. JOHNSON" at that Clay Mountain Road residence in Procious, West Virginia, and the utility company had on file a mailing address for JOHNSON of the same P.O. Box in Maysel, West Virginia, as has previously been referenced in Paragraphs45-47. The date of birth on file with JOHNSON'S AEP account matched the date of birth reflected in the Facebook CyberTip. The West Virginia driver's license number on the AEP account was #XXXXX98.

XI. CONCLUSION

50. Based on the aforementioned information, and my training and experience, your affiant respectfully submits that there is probable cause to believe that the user of the Facebook account Rj Johnson (UID 100044893370664), ROBERT JOHNSON, has committed a violation of Title 18, United States Code, Sections 2252A(a)(1), 2252A(a)(2), and 2252A(a)(5)(B) and that evidence of those offenses, as more fully described in Attachment B, is presently contained in the Facebook account located on the computer system or server in the control of Facebook, Inc, more fully described in Attachment A. Accordingly, your affiant requests Facebook, Inc. be ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

SPECIAL AGENT TERRANCE L. TAYLOR
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

Signed and sworn to by telephonic means
on this 3rd day of August, 2021:

DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with Facebook account: **"Rj JOHNSON"** which bears Facebook User Identification Number ("UID") **100044893370664** and which is stored at premises owned, maintained, controlled, or operated by Facebook, Inc., an electronic service provider that is headquartered at 1601 Willow Road, Menlo Park, CA 94025.

ATTACHMENT B

Description of Items to Be Seized and Searched

I. Information to Be Disclosed by Facebook, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, Inc. ("Facebook"), regardless of whether such information in located in or outside of the United States, including any messages, records, files, logs, or other information that have been deleted but are still available to Facebook or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the account and UID listed in Attachment A:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities December 1, 2020 through present;

(c) All photos and videos uploaded by that account and all photos and videos uploaded by any user that have the target account tagged in them from December 1, 2020, through present, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that account, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(f) All other records and contents of communications and messages made or received by the account from December 1, 2020, through the present, including all

Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the account;

(i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(j) All information about the Facebook pages that the account is or was a "fan" of;

(k) All past and present lists of friends created by the account;

(l) All records of Facebook searches performed by the account from December 1, 2020 through the present;

(m) All information about the user's access and use of Facebook Marketplace;

(n) The types of service utilized by the user;

(o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(q) All records pertaining to communications between Facebook and any person regarding the account or the account's Facebook information, including contacts with support services and records of actions taken.

Facebook is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information To Be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of, among other statutes, Title 18, United States Code, Section 2252A(a)(1), (a)(2), and (a)(5)(B), which relate to the knowing transfer, receipt, distribution, possession of child pornography, to include the following:

(a) Records of any images or videos of suspected child pornography or child erotica, whether uploaded, sent, received, or downloaded by the target account;

(b) Records of any messages, posts, or other communications involving discussions of child pornography, child erotica, the sexual abuse of minors, sexual interest in minors, or sexual relationships between adults and minors;

(c) Records of any groups joined by the target accounts that relate to child pornography, child erotica, the sexual abuse of minors, sexual interest in minors, or sexual relationships between adults and minors;

(d) Evidence indicating how, when, and where the Facebook accounts were accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

(e) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

(f) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.